UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/996,948	11/27/2001	Chinna Narasimha Reddy Pellacuru	50325-0607	2395

29989 7590 04/10/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 04/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/996,948	PELLACURU, CHINNA NARASIMHA REDDY	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6,9,11,12,15-17 and 20-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,6,9,11,12,15-17 and 20-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *01/23/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The office action is in replay to an amendment filed on 01/10/2006.Claims 3-5,7-8,10,13-14,16,18-19 have been cancelled. Claims 2,6,9, and12 have been amended. Claims 30-45 have been added. Claims 1-2,6,9,11-12,15,17, and 20-45 are pending.

Response to Arguments

2. Applicant's arguments, see Remarks, filed 01/10/ 2006, with respect to the rejection(s) of claim(s) 1-29 under U.S.C.102 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Hardjono, Matt and Wesley.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 21,22,25 are rejected under 35 U.S.C. 102(e) as being anticipated by Wesley et al (US Patent No 6,275,859 B1).

5. As per claim 21,25: Wesley teaches a method for encrypting a communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of: sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier (See Fig 1 col 1 line 50 through col 2 line 7); encrypting data based on the encryption key; and multicasting the encrypted data with the identifier to one or more receiving nodes, wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key(See Fig 1 and col 1 line 50 through col 2 line 27).

6. As per claim 22: Wesley teaches a method for decrypting encrypted communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of: receiving from an originating node a multicast that includes encrypted data and an identifier (See Fig 1 and col 1 line 50 through col 2 line 27); identifying the identifier from the multicast (see abstract); sending a request that includes the identifier to an authoritative node for an encryption key used by the originating node to encrypt the encrypted data(See abstract); in response to the request to the authoritative node, receiving the encryption key(); and decrypting the encrypted data based on the encryption key(See Fig 1 and col 1 line 50 through col 2 line 27).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-2,9-12,15,17,30,32-38,40-45 rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (US Patent No 6,643,773 B1) in view of Matt (Pub. No US 2003/0026433 A1).

9. As per claims 1,24,26,28: Hardjono teaches a method/apparatus/a computer-readable medium for facilitating secure communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of: receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes (col 1 lines 41-57 and col 2 lines 3-17);

Hardjono does not explicitly teach in response to the first request, storing the encryption key; creating and storing an association between the encryption key and the identifier; receiving, from at least one second node of the plurality of second nodes, a second receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier; in response to the second request, based on the identifier included in the second request and the association between the encryption key and the identifier,

retrieving the encryption key; and sending the encryption key to the at least one second node for use in decrypting the encrypted data.

However Matt teaches in response to the first request, storing the encryption key (See paragraph 0039,0042); creating and storing an association between the encryption key and the identifier (See paragraph 0009,0039,0042); receiving, from at least one second node of the plurality of second nodes, a second receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier (See paragraph 0009 and 0040); in response to the second request, based on the identifier included in the second request and the association between the encryption key and the identifier, retrieving the encryption key(See 0012-0013); and sending the encryption key to the at least one second node for use in decrypting the encrypted data(See paragraph 0010 and 0040).

Therefore it would have been obvious for one ordinary person in the art at that time the invention was made to employ the teachings method of Hardjono within Matt because it would enhance the security by provides a system for establishing a shared cryptographic key between participating nodes in a network.

10. As per claims 2,30,38: the combination of Hardjono and Matt teach a method/apparatus/ a computer-readable medium wherein: a trusted third party performs the steps of receiving the first request, storing the encryption key, creating and storing the association, receiving the second request, retrieving the encryption key, and sending the encryption key (See Matt 0039-0040 Fig 6 items 606,610,614); the first request is encrypted based on a first public key that is associated with the trusted third

party (see Matt 0010,042); the first request is signed with a first private key that is associated with the first node(See Matt 0049); the first node is a router that acts as a multicast originator; the plurality of second nodes is a plurality of routers that act as multicast receivers the trusted third party is selected from the group consisting of a certificate authority, a key distribution center, a key exchange authority, and a key exchange center(See abstract); the encryption key is selected from the group consisting of a second private key(See abstract, Figs 2,6); a shared key, a pseudo-random string of bits, and a pseudo-random string of characters(See Abstract, Figs 2,6); and the method further comprises the computer-implemented steps of prior to sending the encryption key, encrypting the encryption key based on a second public key that is associated with the at least one second node, and signing the encrypted encryption key with a third private key that is associated with the trusted third party(See 0042-53 HASH,MAC etc).

11. As per claims 9,32,40: the combination of Hardjon and Matt teach further comprising the computer-implemented steps step of: generating the encryption key based on an Internet key exchange protocol with the first node (See Hardjono col 4 lines 50-54).

12. As per claims 11,33,41: the combination of Hardjon and Matt teach further wherein: the first node uses the encryption key and internet protocol security (IPsec) to encrypt the data that is multicast; and the at least one second node decrypts the encrypted data based on the encryption key and Ipsec (See Hardjono col 4 lines 50-54).

13. As per claims 12,34,42: the combination of Hardjono and Matt teach a method further comprising the computer-implemented steps of: storing a first list of nodes (See Hardjono col 4 lines 1-4); in response to the first request, determining whether the first node is included in the first list of nodes: when the first node is included in the first list of nodes, performing the steps of storing the encryption key and creating and storing the association between the encryption key and the identifier, in response to the first request, storing the a second list of nodes(See Hardjono col 5 lines 1-21); In response to the second request, determining whether the at least one second node is included in the second list of nodes(See Hardjono col 1 lines 41-52); and when the at least one second node is included in the second list of nodes, performing the steps of retrieving and sending the encryption key(See Hardjono col 1 lines 41-52).

14. As per claims 17,36,44: the combination of Hardjono and Matt teach a method wherein the identifier is a session identifier (col 1 lines 41-52); the encrypted data is multicast with an originator identifier that is based on an identity of the first node (col 2 lines 3-17); the second request includes an unverified originator identifier (col 2 lines 3-17); and further comprising the computer-implemented steps of: in response to the first request, associating the originator identifier with the session identifier(col 1 lines 41-52); and in response to the second request, determining whether the unverified originator identifier is valid based on the originator identifier and informing the at least one second node whether the unverified originator is valid(col 2 lines 49-55).

15. As per claim 20,37,45: the combination of Hardjono and Matt teach a method wherein the identifier is selected from the group consisting of a hostname, an Internet

protocol address, a media access control address, an Internet security protocol security parameter index, a first string of pseudo-random bits, a second string of pseudo-random characters, a third string of arbitrary bits, and a fourth string of arbitrary characters (See Hardjono col 4 lines 41-66).

16. Claims 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wesley et al(hereinafter referred as Wesley)US Patent No 6,275,859 B1 in view of Turtiainen et al(hereinafter referred as Turtianinen) Pub. No US 2002/0059516 A1.

17. As per claim 23: Wesely teaches a method for a certificate authority to facilitate communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of: receiving, at the certificate authority from a first router that acts as a multicast originator, a first request to register an encryption key, wherein the first request includes a multicast session identifier and a list of authorized multicast receivers, and wherein the first router uses the encryption key to encrypt data based on IPsec and multicasts the encrypted data with the multicast session identifier to a plurality of second routers that act as multicast receivers (See Fig 1 and col 1 line 50 through col 2 line 27); in response to the first request, the certificate authority creating and storing a multicast session certificate that includes the encryption key, the multicast session identifier, and the list of authorized multicast receivers; receiving, at the certificate authority from at least a particular second router of the plurality of second routers, a second request to obtain the encryption key, wherein the second request includes the multicast session identifier; in response to the second request, determining whether the particular second router is included in the list of

authorized multicast receivers(See Fig 1 and col 1 line 50 through col 2 line 27); when the particular second router is included in the list of authorized multicast receivers, based on the multicast session identifier included in the second request and the multicast session certificate, the certificate authority retrieving the encryption key; and the certificate authority sending the encryption key to the particular second router for use in decrypting the encrypted data(See Fig 1 and col 1 line 50 through col 2 line 27).

Wesley does not explicitly teach encrypt data based on IPsec. However Turtiainen teaches use of IPsec in multicast system (0012-0014,0033). Therefore it would be obvious to one having ordinary skill in the art at the invention was made to employ the teachings method of Tuntianinen with the system of Wesley in order to achieve secure communication among multicast group communication.

18. Claims 6,31,39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (US Patent No 6,643,773 B1) in view of Matt (Pub. No US 2003/0026433 A1) and further in view of Yung-Kao Hsu (US Patent No 5982898).

19. As per claims 6,31,39: the combination of Hardjono and Matt teach claim 1 as recited above. Hardjono and Matt don't explicitly teach a method/apparatus/ a computer-readable medium further comprising the computer-implemented steps of: registering a certificate that includes the encryption key and the identifier: in response to the first request, associating an expiration time with the encryption key; in response to the second request, determining based on the expiration time whether the encryption key has expired; and when the encryption key has expired, revoking the certificate.

However Yung-Kao Hsu teaches computer-implemented steps of: registering a certificate that includes the encryption key and the identifier: in response to the first request, associating an expiration time with the encryption key (col 3 lines 19-37); in response to the second request, determining based on the expiration time whether the encryption key has expired (col 3 lines 19-37); and when the encryption key has expired, revoking the certificate (col 3 lines 19-37).

Therefore it would have been obvious for one ordinary person in the art at that time the invention was made to employ the teachings method of Yung_Kao Hsu within Hardjono and Matt because it would secure communication channels by using a public key cryptosystem for authenticating a user.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

22. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 5712738300. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

23. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Fikremariam Yalew
03/16/06

Art Unit 2136

CHRISTOPHER REVAK
PRIMARY EXAMINER